Testimony Presented on Behalf of
Gas Technology Institute

by

Dr. William F. Rush
Institute Physicist
Gas Technology Institute

Presented before the U.S. House of Representatives
Subcommittee on Economic Security, Infrastructure Protection

Hearing on SCADA and the Terrorist Threat: Protecting the Nation's Critical Control Systems

Tuesday, October 18, 2005
Washington, D.C.

INTRODUCTION

Good afternoon Mr. Chairman and members of the Subcommittee. Thank you for the opportunity to address you today on this important topic. My name is Bill Rush and I hold the position of Institute Physicist with the Gas Technology Institute (GTI), where I have worked in the field of natural gas technology research and development for 27 years. GTI is a not-for-profit Research and Development institute headquartered in Des Plaines, Illinois. I also am the Chairman of the American Gas Association's SCADA Encryption Working Group. The American gas industry has charged this group with developing cryptographic protection for gas, water, and electric SCADA communications.

The focus of my testimony today is to update you on the steps the American Gas Association AGA, GTI, and many other organizations have begun to take to protect SCADA communications from cyber attack. At the conclusion of my remarks, I will provide recommendations to the Subcommittee on what actions can be taken to further advance the security of industrial control systems for critical infrastructures.

SCADA SYSTEMS ARE OFTEN VULNERABLE TO CYBER ATTACK

Supervisory Control And Data Acquisition (SCADA) systems are an important component of critical infrastructure. SCADA systems can be thought of as the "remote control" part of most gas, water, electric, and oil pipeline systems. SCADA Remote Terminal Units (RTUs) read the pressures, voltages, temperatures, and flows at critical points throughout the transmission and distribution portions of these critical infrastructure networks and transmit this real-time data back to central control rooms. They also operate valves, circuit breakers, and switches and are thus critical equipment for control of the systems. This remote control of unmanned facilities provides quick response to changing situations, while providing cost-effective operations of a multitude of critical equipment and stations, spread over a large geographic area. Many SCADA RTUs have "maintenance ports" that enable operators to change critical system parameters remotely, open or close valves or breakers, or download new firmware. There are strong similarities among gas, water, electric, sewage, and oil SCADA systems. Process automation and control systems used in other critical infrastructure applications, such as oil refineries and chemical plants, may not have the long-distance aspects of SCADA, but share many other characteristics.

The cost constraints under which SCADA systems operate determine many of their security-related characteristics. Because SCADA systems are expensive to replace, they have long life times – typically between 10 and 20 years. Consequently, many systems now in service have been there for a long time and will remain as legacy systems for some time to come. Consequently, today's SCADA systems are often based on technology which is a decade old. In particular, many of these systems operate at relatively low communication speeds over telephone modems, speeds which most Internet users of today find unacceptably slow.

Because these systems were designed before critical infrastructure security was a major concern, they often have significant vulnerabilities to unauthorized electronic operations, referred to as "cyber attacks". Many of the systems do not have effective password protection for access control or encryption for confidentiality of data and commands. When they use dial-in telephone modems, they often can be hacked from any computer with a phone modem. When the SCADA system uses radio communication, the radio waves can often be detected and altered by a third party with an appropriate, commercially available receiver/transmitter. The question confronting skilled cyber attackers is less "Can we enter the system?" and more "How long will it take us to penetrate it?" The North American Electric Reliability (NERC) is concerned about the ability of an attacker to use the maintenance ports to attack SCADA systems by making unauthorized changes in critical system parameters. Information on American SCADA systems has been found on captured Al-Qaeda computers.

Cyber attacks are not simply minor incidents involving mildly annoying hackers, but can have significant operational, economic, and safety consequences. A single example that underscores this point is the Soviet Union's use of stolen American SCADA software during the 1980's. This code – which had been deliberately modified to cause harm to a SCADA system - led to physical damage to the Soviet SCADA system resulting in an explosion large enough to be photographed from space and estimated at 3 kilotons TNT equivalent. (See "At the Abyss: An Insider's History of the Cold War", Thomas C. Reed, Ballantine Books, New York, 2004.) To put the 3 kiloton number into perspective, the Murrah Federal Office Building bombing in Oklahoma City was estimated at 0.002 kiloton and the Hiroshima nuclear bomb was between 14 and 20 kilotons. The salient point is that it clearly is possible to cause significant physical damage to critical infrastructure if the SCADA code can be modified.

AGA 12 IS A STANDARD TO PROTECT SCADA FROM CYBER ATTACK

Three weeks after the 9/11 attack, AGA chartered a working group to develop a comprehensive standard that would use cryptography to protect SCADA communications from cyber attack. This standard has been designated "AGA 12". When it is completed, it will be a comprehensive approach to SCADA cryptography. The charter instructed the working group to develop a recommended practice for the gas industry and to include water and electric SCADA systems as well. This approach also applies to sewage and oil pipeline SCADA systems. This effort has made such significant progress that we are now field testing commercial prototypes of products that use cryptography to protect SCADA communications.

As a standard, AGA 12 has several significant characteristics. First, it is an open consensus standard that is designed to produce interoperable cryptographic products. "Open" means that anyone can use the standard to build equipment without needing to pay a royalty or licensing fee. Open here also refers to the process by which anyone with an interest in the topic can participate in developing the document. The working group included this requirement to encourage market competition to drive costs down, since no one has a monopoly position. The open-source code for implementing AGA 12 is available for free on the Internet. AGA 12 is a consensus standard because the working group develops consensus among its members and the AGA membership as well that its recommendations are indeed a sound practice. Finally, the standard specifies a minimum level of interoperability among products made by different manufacturers. Thus, users will have a choice of suppliers. The standard also assures that new products will remain compatible with earlier versions. Finally, AGA 12 provides strong protection; it is based on well-established NIST encryption standards and has been examined for its ability to protect against a wide variety of attacks.

AGA 12 is a suite of 4 documents, designated Parts 1 through 4. The four documents address different aspects of SCADA communication protection.

AGA 12, Part 1 (AGA 12-1) summarizes cyber security policies, the background of the cyber security problem, and a procedure for testing cryptographic protection systems. This document educates SCADA operators on the need to do a risk assessment and recommends an approach for those utilities whose risk assessment reveals a need to protect their systems with cryptography.

AGA 12-2 is a detailed technical specification for building interoperable cryptographic modules to protect SCADA communications for low-speed legacy SCADA systems and dial-up maintenance ports.

AGA 12-3 will describe how to protect high speed communication SCADA systems.

AGA 12-4 will describe how to build next generation SCADA systems so that their cryptography will be compatible with the legacy systems; this will ease the transition to the newer designs.

Parts 1 and 2 are close to completion. Parts 3 and 4 are in the planning stage.

Figure 1 illustrates both the configuration of a SCADA system and the scope of AGA 12. On the left is the Control Room, which is manned around the clock and where critical operational decisions are made. On the right is the "Remote Terminal Unit" (RTU), which is typically unmanned and controls the sensors and actuators that operate the critical infrastructure. Both the Control Room and the RTU are assumed to be secure. The AGA 12 working group deals only with the issues of security of messages while they are in transit over an insecure network and leaves to others the responsibility for securing the rest of the system.

It is important to recognize that while cryptographic protection of SCADA communications is an important weapon in the arsenal of tools that can protect SCADA, it is only one tool among many that are needed. Cryptography can not provide any protection at all against many kinds of attacks. In particular, it does not protect against jamming or breaking the communication line, against physical attacks, or against many kinds of insider attacks. Nor does it protect local facility control systems[1] that are often connected to SCADA systems, and usually offer additional independent vulnerabilities to cyber attack. These issues are being addressed by literally dozens of groups working in the security area. While I am focused only on the AGA 12 effort, I am pleased to report that there are so many security initiatives under way that coordinating their work is a major challenge. I would call your attention to both the Department of Energy's Roadmap to Secure Control Systems in the Energy Sector and the Department of Homeland Security's Process Control Systems Forum as good examples of how the Government is working effectively with the private sector to advance and coordinate the many security efforts that are now under way. I also call your attention to the Instrumentation, Systems and Automation Society's (ISA) ISA SP99 committee, "Manufacturing and Control Systems Security". This is a broad industry wide automation and control systems security standards effort that has published over 150 pages of guidance on how to establish automation systems

[1] These local control systems are often referred to as Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), safety systems, and by many other names. Regardless of the name, cyber defenses are only as strong as the weakest link in the chain It is important to apply appropriate countermeasures whenever risks are unacceptable..

security programs and available technologies to deal with unacceptable risks. Finally, the National Institute of Standards and Technology (NIST) has produced many standards on which AGA 12 has relied and operates the Process Control Security Forum (NIST PCSRF) which continues to advance putting the cause of cyber security on a firm basis.

AGA 12 SPECIFIES CRYPTOGRAPHY TO PROTECT SCADA COMMUNICATIONS

AGA 12 uses cryptography to protect SCADA communications. Figure 2 illustrates the basic idea of how this works. Data and commands ("Open Switch" in this figure) originate inside of a secure facility, as illustrated in Figure 1. Prior to leaving the secure facility, the data or command is sent to a "SCADA Cryptographic Module" (SCM) which encrypts it. Essentially, this encryption step changes the message so that it can no longer be read by anyone without a special number, called a key. In operation, the encrypted message is sent over the insecure network in an unintelligible form. When it arrives at the designated secure facility, the key is used to decrypt the message, returning it to its original meaning, "Open Switch".

The AGA 12 standard has gone to great length to assure that encrypted messages are very difficult for potential attackers to use to harm a system that uses SCADA. This "link encryption" approach has been used successfully for many years by the financial community to secure its transactions. While this discussion has only considered making the message hard to read, AGA 12 also makes it difficult to alter, forge, or record and replay a message. An important issue associated with AGA 12 is how these secret keys are managed. The keys must be changed periodically to prevent their being guessed or compromised. Different keys are used for employees with different responsibilities and different levels of authority. The authorization to use keys must, for example, be changed if an employee leaves. It is important to be able to do this without the expense of visiting the many distant sites that may be controlled by the SCADA system.

Because of the long life of SCADA systems, the owners and operators of these systems urged the working group to focus first on the challenging problem of protecting legacy systems. Focusing on next-generation SCADA systems first would leave the legacy systems unprotected for many years. Protecting legacy systems, however, required developing cryptographic modules that will support most of the roughly 150 types of existing SCADA systems, each of which has a different "SCADA language" and which operate at different communication speeds and over a wide variety of communication media (such as telephone, radio, and microwave.) The next steps are to develop the same standard protection for high speed and next generation SCADA systems.

AGA 12 HAS MADE RAPID PROGRESS FOR A STANDARD

AGA 12 has made rapid progress, given the constraints that an open group is developing a consensus standard. This is a process that is generally slow for two reasons. First, developing consensus among users, manufacturers, and cryptographic experts on a difficult technical task is a challenging task. Each group has different needs and understanding levels for the standard. Second, most standards development efforts are all volunteer activities. This limits the rate of progress to what can be accomplished in an overload or spare time mode by people with full-time job responsibilities.

Those of us who have participated in the AGA 12 process are proud of the success we have achieved, for this is no longer just a paper standard. AGA 12 Part 1 is in the final stage of balloting prior to being adopted as an industry recommended practice. Two manufacturers are offering or soon will offer cryptographic modules that comply with AGA 12, Part 2. Early versions of this equipment have performed well in field tests at actual gas companies. AGA 12 has entered the field test stage at least 2 years ahead of any other group developing an open standard for cryptographic hardware.

MANY GROUPS HAVE CONTRIBUTED TO THE SUCCESS OF AGA 12

Many groups have contributed to the success of AGA 12. No single group did more to accelerate the work of AGA 12 than the Technical Support Working Group (TSWG), a part of the Combating Terrorism Technology Support Office. TSWG began support of cryptography for SCADA systems with a project at GTI in 1998, well before terrorism was recognized as a threat. While as previously mentioned, most standards groups operate on an all volunteer basis, TSWG funded GTI to provide full-time support by several people to work on AGA 12. This allowed us to debate approaches, build models of the various ideas, test to see what does and what does not work, write our results into the emerging standard, and begin the cycle anew with a debate on the next issue.

In addition to TSWG support, several other government agencies have contributed to the progress of AGA 12. The National Institute of Standards and Technology provided funding to help develop a standard test methodology for evaluating how much cryptography slows communications in network. Sandia National Laboratories evaluated the security level of the first version, work which led to several significant improvements to AGA 12. Pacific Northwest National Laboratory conducted a preliminary test on the impact of AGA 12 on communication speed. Under DOE sponsorship, both of these laboratories continue to do work on the security and performance of the AGA 12-compliant cryptographic modules. These National Laboratory tests are particularly important to the private sector's acceptance of the AGA 12 standard as both secure and functional.

In addition to government support, industry groups have helped. Both AGA and the American Water Works Association Research Foundation (AWWARF) have provided funding and substantial in-kind support for the AGA 12 standard. GTI and the Gas Research Institute have funded the AGA 12 work as well.

Many private companies also supported the AGA 12 project. These include Cisco, OPUS Publishing, SafeNet Mykotronx, TecSec, Schweitzer Electronic Laboratory, Thales e-Security, and Weston Technology. Peoples Energy (Chicago) and Detroit Edison have also been supportive and contributed extensively to the working group's understanding of the needs of SCADA operators.

DESPITE REMAINING WORK, AGA 12 HAS SLOWED SUBSTANTIALLY

Although significant work remains to be done to complete the AGA standard, progress stopped in May of 2005 when TSWG funding ran out. TSWG is an organization which only funds prototype developments until they prove successful, at which time funding is to be provided by other organizations. DOE has supported Sandia and Pacific Northwest National Laboratory to evaluate the security level of the standard and the speed of its encryption, respectively. In October, DOE provided limited funding for GTI to complete some field testing and write up the existing version of AGA 12-2 as a document that is in a suitable format for ballot. This 5 month hiatus significantly reduced the momentum of the AGA 12 project. Largely as a result of these delays, one of the three manufacturers that originally committed to produce AGA 12 modules has stopped work on this project.

Regrettably, AGA 12 became a victim of its own success. Given that it is well ahead of any other hardware development of cryptographic protection and manufacturers are developing products, it appears that market forces have now taken over and there is no further role for government support.

The apparent success of AGA 12 obscures the additional work that is required. This includes several topics that – while of great importance to the success of the AGA 12 effort – are difficult to appreciate. These include the following:

- Conformance testing – While the AGA 12 standard will be validated by at least two National Laboratories, SCADA system owners and operators need a "seal of approval" to verify that the particular products they are considering buying actually do conform to AGA 12 requirements. There is no existing set of tests that is recognized as providing this assurance.
- Next generation design – Because AGA 12, Part 2 is a retrofit solution for legacy systems, it is the most expensive and least effective approach to the cryptographic protection to SCADA systems. Incorporating this protection into products at the time of manufacture is estimated to be less than half as costly as adding it after it is in the field. It is critical, also, that the next generation systems be able to interoperate with the units that have already had cryptography added.
- Large scale pilot test – While the laboratory and small-scale field tests that have been completed and will be done in the near future will validate that AGA 12 does work in the field, this is not a full scale pilot test. Several parts of AGA 12 that will function well during a small scale test may prove problematic for larger scale installations. Key management is a good example. Another is the possibility that network congestion problems might manifest themselves when many of the messages are encrypted, but will be invisible in small scale tests. SCADA operators are more likely to feel confident in a system that has been tested in a full-scale pilot than in a system that has only been tested on a small scale.
- Key management – Good cryptographic practice requires that the keys that decrypt the encrypted data and commands be changed periodically. This "key management" must be

done remotely to be cost effective, since the wide geographic extent of SCADA systems prohibits visiting sites to change keys if a strike occurs or if an employee leaves.

- Forensics and diagnostics – While it is important that AGA 12 be able to protect SCADA systems from attack, it is also desirable that these systems detect attacks that are under way, inform the operator of the attack, and gather possible forensic information that will facilitate the detection, identification, arrest, and prosecution of system attackers. Although AGA 12 contains some features that lay foundations for this type of work, it is far from complete.
- Management port – The management port requires some additional features that are different from those required to send data and commands.
- Coordination of security standards – It is important that standards groups establish and maintain contact with one another. There are estimated to be approximately 100 groups currently developing cyber security related standards. There is very little contact among these groups, an undesirable situation likely to lead to duplication of effort and conflicting standards that no manufacturer will follow.
- High speed networks – While AGA 12's early focus on the protection of low speed legacy SCADA systems is appropriate in providing protection to the large installed base of these systems, it is also clear that many of the newer systems will use higher speed communication links, such as the Internet. This requires that we be able to maintain as much interoperability as possible between the low and high speed networks.

SEVERAL GOVERNMENT STEPS WILL ADVANCE SCADA SECURITY

In summary, we make the following recommendations

- Make sure that there is funding for R&D and strong industry-government partnerships to develop protection of the Nation's critical infrastructure against cyber attacks. Progress is being made – the key to moving forward is to continue R&D efforts and partnerships.
- Prevent loss of momentum by avoiding funding interruptions in on-going programs.
- Continue the coordination efforts (such as the DOE Control Systems Roadmap and the DHS Process Control Systems Forum) which are key elements of growing coordination between the government and industry and also vital to coordination among different infrastructures. These two programs are models for how to coordinate across a wide area.
- Support continued development of AGA 12. In particular, work should be completed to develop key management, establish conformance tests, do a large-scale pilot test, specify a next-generation design, secure high-speed networks in a manner compatible with the low speed networks, and develop forensics and diagnostics to detect and foil attacks.
- Support selected other standards development efforts. While our focus here has been on AGA 12, it is important to recall that this is only a small part of the total SCADA security requirements. Both the ISA SP99 and the NIST PCSRF efforts are noteworthy. Many of these other standards groups labor on an all volunteer basis on other critical requirements of significance as great as that of AGA 12. This all volunteer pace will not lead to rapid development of required standards.

Mr. Chairman, we applaud your focus on securing our critical infrastructure, especially in the area of SCADA protection. This concludes my prepared statement. I would be pleased to respond to any questions you or other Members of the Subcommittee may have.

List of Acronyms

AGA – American Gas Association

AGA 12 – American Gas Association Report No. 12, “Cryptographic Protection of SCADA Communications”

CM – Cryptographic Module

DOE – Department of Energy

EPRI – Electric Power Research Institute

GTI – Gas Technology Institute

ISA – Instrumentation, Systems and Automation Society

ISA SP 99 – ISA Special Publication 99, “Manufacturing and Control Systems Security

NERC North American Electric Reliability Council

NIST – National Institute of Standards and Technology

PCSRF – Process Control Security Research Forum

RTU – Remote Terminal Unit

SCADA – Supervisory Control And Data Acquisition

SCM – SCADA Cryptographic Module

TNT – Tri-Nitro Toluene (dynamite)

TSWG – Technical Support Working Group, part of the Combating Terrorism Technology Support Office

FIGURES

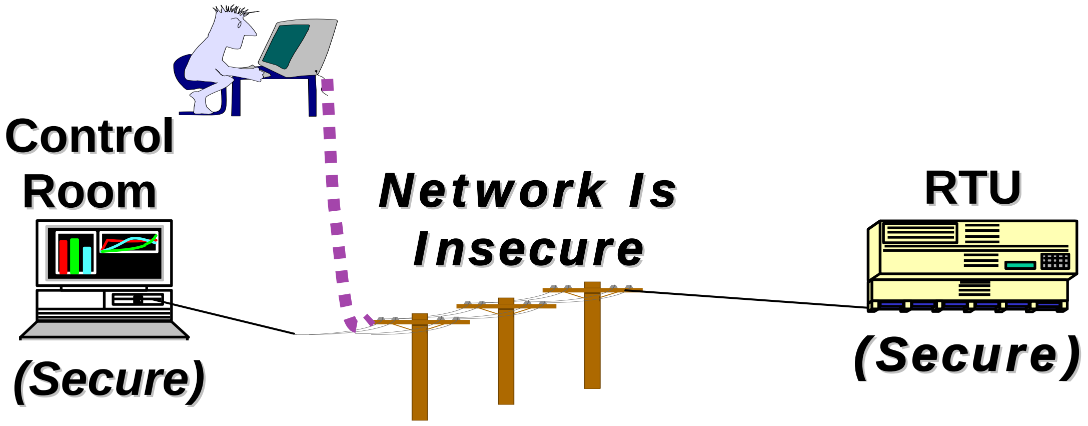

Figure 1 – AGA 12 assumes both the Control Room and the Remote Terminal Unit (containing the sensors and actuators) are secure

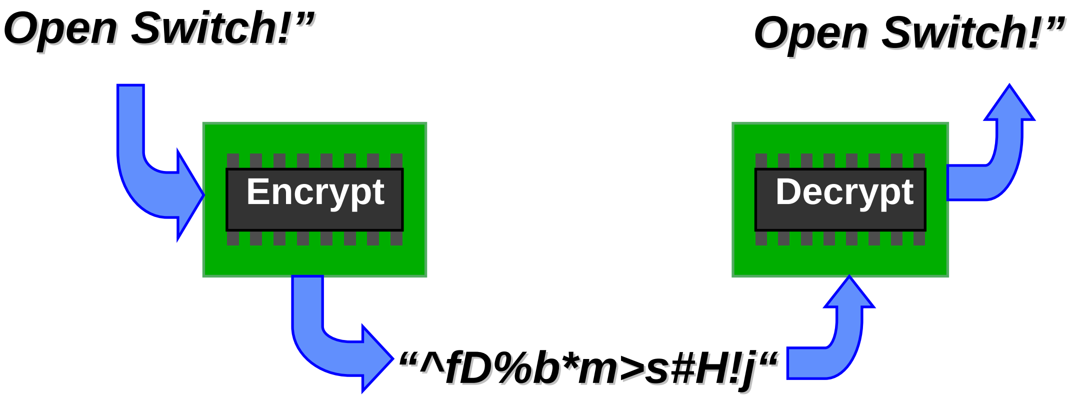

Figure 2 – AGA 12 specifies that the messages (Open Switch here) are encrypted inside a secure facility so that they are “scrambled” and can not be read. They are thus unreadable while they are on the insecure network, but can be decrypted and read properly when they are delivered to the second secure site.